

Amendments to the Specification:

Please rewrite paragraph [0001] as follows:

[0001] This is a continuation of copending application number 09/699,884 filed on October 30, 2000, now United States Patent 6,678,707, which is hereby incorporated by reference herein.

Please rewrite the Abstract as follows:

ValuesIn one embodiment, values are retrieved from a number of MISRs which are coupled to a number of microprocessor buses, and a random number is generated based on the retrieved values. In another embodiment, a built-in self-test (BIST) local block of a microprocessor is assigned a major address, and each of a number of multiple input shift registers (MISRs) in the BIST local block is assigned a minor address. An instruction to turn on and initialize the MISRs is then issued, and a request to read the MISRs is issued in response to a request for an encryption key. The MISR readings are then XORed with each other, and with historical readings, if any, to generate an encryption key.